REMARKS

A. Drawing Amendment

In FIG. 5, reference number 136 has been added to identify the verification engine. Support for the amendment can be found, for example, on page 6, line 20, of the specification as originally filed. Approval of the drawing change is respectfully requested. No new matter has been added.

B. Support For Specification Amendments

Support for the amendment to the paragraph spanning from page 5, line 12, to page 6, line 2 of the specification as originally filed can be found, for example, on page 6, line 11. Support for the amendment to the paragraph spanning lines 8-23 of page 7 of the specification as originally filed can be found, for example, on page 4, line 13. Approval of the specification amendments is respectfully requested.

C. Support For Claim Amendments

Support for new claims 15-33 is found on at least pages 5 through 7. Approval of the claim amendments is respectfully requested.

D. The §103 Rejections

Claims 1-14 were rejected under 35 U.S.C. §103(a) as being unpatentable over the combination of U.S. Patent Application Publication No. 2001/0027519 to Gudbjartson et al. ("Gudbjartson") in view of newly cited U.S. Patent Application Publication No. 2001/0044843 to Bates et al. ("Bates"). The Applicants respectfully disagree and traverse these rejections for at least the following reasons.

As noted, claims 1-14 have been cancelled. Accordingly, the Applicants believe the rejection of these claims is now moot, and respectfully request withdrawal of the rejections.

E. New Claims 15-32

As set forth in Applicants' previous responses (repeated here briefly) Gudbjartson does not disclose or suggest allowing a client to access a list of pre-authenticated application servers associated with a client identifier as in claims 15 and 24. The Examiner acknowledges as much in the Office Action (page 4). To make up for the deficiencies in Gudbjartson, the Examiner relies on newly cited Bates.

Before turning to Bates the Applicants note that Gudbjartson does not appear to disclose or suggest other features of claims 15 and 24. For example, both claims include the features of: the reception of a pre-authentication request to establish a communication link between the client and a selected application server in the list; providing the selected application server with information, including the client identifier, for authenticating a link request sent directly from the client to establish the link between the client and application server; and providing the client with information, including the client identifier, to forward the link request directly to the selected application server to establish the link between the client and application server.

Instead, Gudbjartson appears to set up a link between two users called a "data collector" 109 and "data analyzer" 110 in such a manner that the identity of one or both users remains anonymous. There does not appear to be a link established between one of the users 109, 110 and an application server. At most, there appears to be a "secure connection" established between a user 109 and communications module 107, not application data module 113. Yet further, the links that Gudbjartsen may establish do not appear to be authenticated using a client identifier.

Turning now to Bates, according to new claims 15 and 24 the link that is established between the user and application server is created using a link

request that is sent directly from a client to the application server. Bates does not disclose or suggest this feature.

According to Bates, a connection between one or more server computers and a user is created through the use of a helper PC 202 and a switch control computer 200. In more detail, a user at location 46 inputs a running list of server computers for which connections are desired to the helper PC 202, the running list being a subset of a list of server computers which the user is authorized to access. The helper PC 202 communicates the running list to the switch control computer 200. The switch control computer 200 then acts as a liaison between the server computers 20 and the user location 46 to establish respective communication paths. The result is that the user at location 46 is connected to one or more of the server computers 20. (see Bates, paragraphs [0053] through [0055]).

At no point, however, does Bates teach that the switch control computer 200 provides any one of the server computers 20 with information for authenticating a link request directly from the user location 46. Nor does Bates teach that the switch control computer 200 provides the user location 46 with information for forwarding a link request directly to any one of the server computers 20. Rather, the switch control computer 200 stays involved as a liaison until the communication links are established. Accordingly, the user location 46 is not capable of directly communicating a link request to any of the server computers 20. In sum, the noted feature of claim 15 is missing from Bates.

Claims 16-23 and 25-32 depend from claims 15 and 24, respectively, and similarly distinguish over each of Gudbjartson and Bates by their dependency.

F. Conclusion

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact John E. Curtin at the telephone number listed below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 50-3777 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

CAPITOL PATENT & TRADEMARK LAW FIRM, PLLC.

By /John E. Curtin/
John E. Curtin, Reg. No. 37,602
P.O. Box 1995
Vienna, Virginia 22183
(703) 266-3330

ATTACHMENT FOR SPECIFICATION AMENDMENTS
REPLACEMENT PARAGRAPHS
MARKED-UP VERSION

Please replace the paragraph spanning from page 5, line 12, to page 6, line 2 of the specification as originally filed with the paragraph below:

Accordingly, the hypertext report provides a user interface 128 that may be used by a client when the hypertext document is loaded by a conventional web browser of the type such as Explorer published by Microsoft or Navigator published by Netscape. The user interface 128 when used on a client having a conventional graphical user interface such as Microsoft Windows or Apple Macintosh OS. may appear as a separate window that can be accessed when needed by a user on the client. Using the HTML language it will be appreciated that a number of user interface configurations may be ~~maybe~~ used including, but not limited to, pull-down menus or hypertext listings. Once the document has been sent to the client, no further authentication by the user is required to access the application servers contained in the listing. This user interface provides a great advance over existing, authentication methodologies as the user does not have to provide a separate authentication for each of the application servers. Furthermore, it will be appreciated that the authentication administration can be handled by a single server rather than having separate authentication administration for each of the application servers. The client's communication with the authentication server 111 may include a Secure Socket Layer (SSL) session link, cookies or other conventional security measures that may be used to verify continued communication from the client to the authentication server.

Please replace the paragraph spanning lines 8-23 of page 7 of the specification as originally filed with the paragraph below:

If the verification is cleared, a Uniform Resource Locator (URL) is generated containing a unique address for the client to access the application and further includes session assignment information that is encrypted by the verification engine prior to transmittal. The special URL is then transmitted to the Authentication Server illustrated by line 140 which in turn forwards the URL directly to the Client illustrated by line 142. Once received by the client, the URL is addressed back to the application server directly from the client along with the encrypted session information initiating the communication link 130. ~~134.~~ The application server again decrypts the session information and verifies that the URL request was transmitted from the IP address of the client 102 originally transmitted to the application server by the authentication server. The application server also verifies that the session timeout time is still valid. The application server then establishes the trusted communication link 134 directly with the client. The trusted communication link 134 may include security such as an SSL communications link or a cookie containing the relevant session information may be placed on the client's computer. The cookie is used by the application

to verify the user and provide other information relevant to the session such as a session time-out information. The URL then redirects the Client to the application page of the web site.